TABLE OF CONTENTS

SECTION **PAGE**

LIST OF FIGURES

FIGURE **PAGE**

SECTION 13
SECURITY DEVICES

This section describes the requirements for security devices that will be on the Approved Products List (APL). This version of this section contains requirements for firewalls (FWs), Intrusion Prevention Systems (IPSs), Network Access Control, Wireless Internet protocols (IPs), and Virtual Private Network (VPN) devices. Future updates to this section will expand on the devices discussed.

13.1 PHYSICAL SECURITY

Physical security is the responsibility of the installing Base/Camp/Post/Station (B/P/C/S). Essentially, two sets of requirements are associated with a complete Unified Capabilities (UC) system. The end points [i.e., PCs, End Instruments (EIs), Classified Provider Edge (C-PE)] have one set of physical security requirements while the network [i.e., Local Area Network (LAN) switches, security devices, and routers) and signaling products (i.e., Session Controller (SC), Multifunction Softswitch (MFSS), Softswitch (SS), and Media Gateway (MG)] require another set of requirements. A full definition of physical security requirements is beyond the scope of this section.

13.2 SECURITY DEVICES SECURITY DESIGN

Security devices use a defense in-depth approach based on best commercial practices. The product security defenses are categorized as follows and are discussed in Section 4, Information Assurance:

- User Roles.
- Hardened operating systems.
- Auditing.
- Application security.
- Redundant systems.

Additional defenses may be added dependent on the specific threats associated with a product.

The requirements in this section describe those requirements necessary to ensure that the separation of information is maintained and that the network managers are able to be aware of attacks against the network, configure the devices to protect against those attacks, and provide data to perform forensic activity on security-related incidents.

13.3 NETWORK SECURITY DESIGN

One of the principal tenets of any Information Assurance design is the separation of components (i.e., traffic, appliances, and users) and/or services from each other based on their characteristics.

A converged network requires the opposite, in that appliances within a converged network may service the voice, data, and video applications. As a result of this conflict, the interactions between the various component segments must be controlled to ensure that an attacker that gains access to one segment cannot gain access to nor affect the other segments. In addition, interaction control between various segments is used to prevent configuration or user errors in one segment from affecting other segments. The actions of normal users of converged network services must not affect the other services, specifically the voice service. The principal mechanisms that are used within this design for segmenting the network are Virtual LANs (VLANs), segmented IP address space or subnets, and VPNs, and are used in combination with filters, access control lists (ACLs), and stateful packet inspection firewalls [Voice and Video over IP (VVoIP) stateful firewalls] to control the flow of traffic between the VLANs and VPNs.

Figure 13.3-1, Notional Example of Voice and Data ASLAN Segmentation, presents the simplest type of converged LAN with only voice and data applications. Separate VLANs are established between voice and data applications and the Layer 3 switches are responsible for providing access control between the different VLANs using filtering techniques, such as ACLs. In this type of deployment, appliances are classified as VVoIP appliances or data appliances and it may be possible to avoid deploying appliances that service both VVoIP and data appliances. At the Customer Edge (CE) Router (CE-R), separate VPNs may be established, if necessary, to segment the voice traffic from the data traffic as the packets transit the Defense Information Systems Network (DISN) Wide Area Network (WAN). In addition, VPNs may be used to extend the local enclave to remote offices of the same organization, telecommuters, and travelers. Also, the VVoIP traffic is routed from the CE-R to the Provider Edge (PE) Router along the same path as the non-VVoIP traffic. The only connection to the Public Switched Telephone Network (PSTN) is through a Time Division Multiplexing (TDM) interface using Primary Rate Interface (PRI) or Channel Associated Signaling (CAS) so that there is no interaction between the VVoIP system and commercial VVoIP IP networks. Moreover, it is important to note that the SC has two separate interfaces: one for local Network Management (NM) and a second for the Voice over IP (VoIP) end-to-end (E2E) NM traffic.

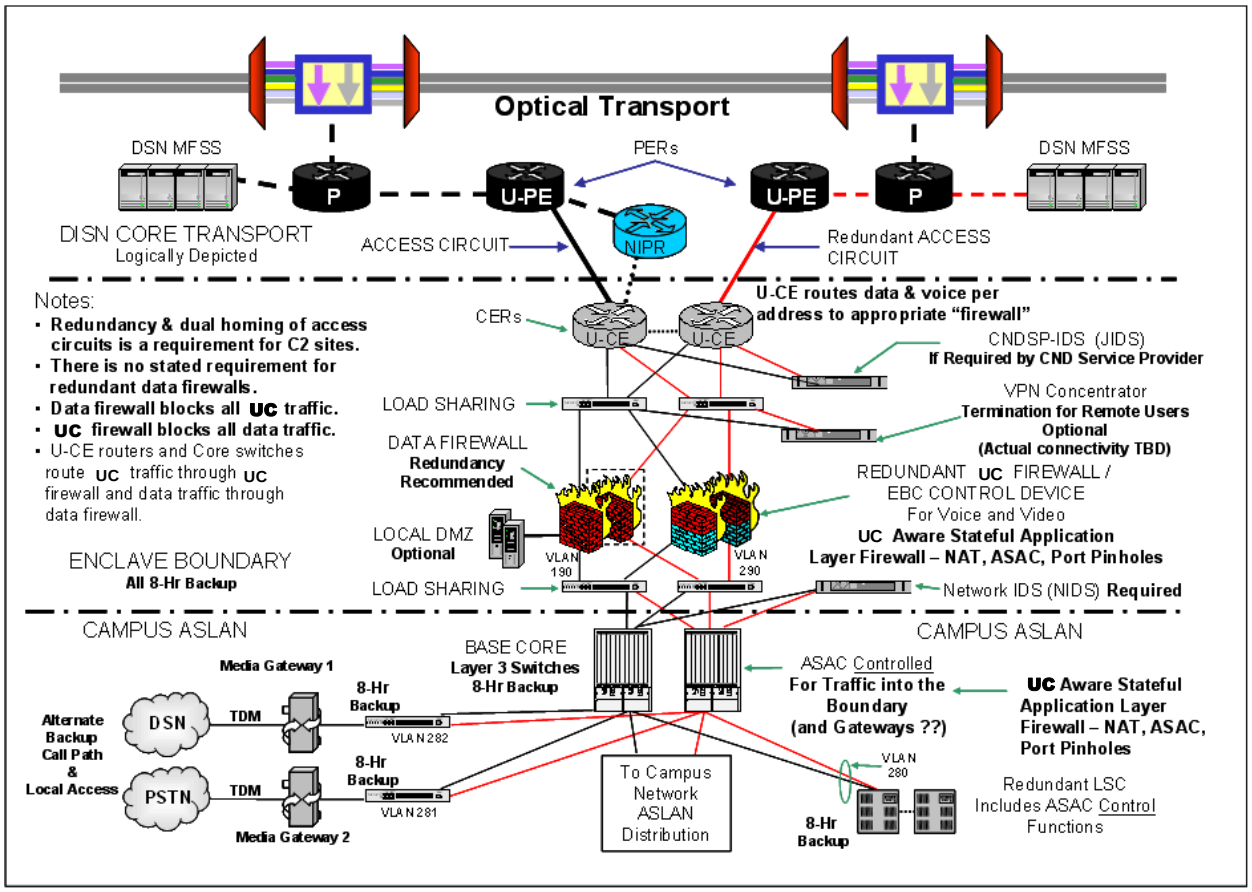

Figure 13.3-1. Notional Example of Voice and Data ASLAN Segmentation

13.4 REQUIREMENTS DEVELOPMENT CONCEPT

Based on the UC Information Assurance design, threats, and countermeasures, a set of derived requirements were developed for security devices. Different vendors combine different functions into their appliances to meet the requirements of a particular type of product. For the purposes of the Unified Capabilities Requirements (UCR), the requirements are levied on the individual security devices, as applicable, to secure the entire product. It is understood that the Information Assurance design provides a high-level description of how the security devices interact in a secure manner. In addition, the appropriate Security Technical Implementation Guidelines (STIGs) will further clarify how the Information Assurance design and requirements are implemented on the appliance. This section is intended to provide a level of security requirements consistent with the level of security requirements defined for the UC, but adapted for the unique Department of Defense (DOD) UC environment consistent with the requirements in the UCR.